AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method for capturing ~~illegal and undesired~~ behavior for network components and for interactions between components comprising:

~~specifying~~ accessing first data that defines one or more states and state transitions for ~~one or more components~~ a particular component or ~~interactions~~ interaction between a particular two or more components,

wherein ~~specifying includes specifying~~ the first data defines at least one composite state transition, each of said composite state transition comprising multiple state transitions; and

~~when a~~ in response to the particular component or interaction between ~~a~~ the particular two or more components ~~enters~~ entering a particular state or state transition, generating a notification corresponding to the particular state or state transition,

wherein the particular state or state transition is one of the one or more states ~~or~~ and state transitions.

2. (Previously Presented) The method recited in claim 1, wherein the one or more states are specified based on thresholds.

3. (Original) The method recited in claim 1, wherein the notification is an event.

4. (Previously Presented) The method recited in claim 1, wherein the particular component or interaction between the particular two or more components is a component, and wherein the step of generating the notification comprises generating the notification by the component.

5. (Currently Amended) The method recited in claim 1, wherein the particular component or interaction between the particular two or more components is an interaction between the particular two or more components, and wherein the notification is generated by at least one of the ~~the~~ particular two or more components.

6. (Original) The method recited in claim 1, further comprising the step of:
reporting the notification to a network management system.

7. (Previously Presented) The method recited in claim 1, further comprising the step of:
detecting that the particular component or interaction between the particular two or more components has entered the particular state or state transition; and
wherein said notification is generated in response to said step of detecting.

8. (Currently Amended) The method recited in claim 7, wherein, the step of detecting is performed by an agent, said agent being different than the particular component.

9. (Canceled)

10. (Previously Presented) The method recited in claim 1, further comprising the step of polling the particular component or the particular two or more components to determine that the particular state or state transition has occurred.

11–14. (Canceled)

15. (Currently Amended) The method recited in claim ~~11~~ 48, wherein the set of one or more illegal states or state transitions comprises a state associated with an authorization violation ~~and~~ or an authentication forgery ~~are defined as illegal states~~.

16. (Currently Amended) The method recited in claim ~~12~~48, wherein the set of one or more undesirable states or state transitions comprises a state associated with a sudden ~~QoS~~ quality of service degradation or a violation of a service level agreement ~~is defined as an undesired state~~.

17. (Previously Presented) The method recited in claim 1, further comprising the step of examining multiple notifications to deduce one or more trends regarding the network.

18. (Previously Presented) The method recited in claim 17, wherein the step of examining multiple notifications comprises examining notifications for stable-behavior in a threshold value for a particular trend.

19. (Previously Presented) The method recited in claim 17, wherein the step of examining multiple notifications comprises examining notifications for increases or decreases in a threshold value for a particular trend.

20. (Currently Amended) A computer-based system for capturing ~~illegal and undesired~~ behavior for network components and for interactions between components, the system comprising:

one or more network components, each network component configured to

spontaneously generate notifications when specified states and state transitions occur involving the network component,

wherein the specified state and state transitions include one or more composite state transitions, each of said composite state transition comprising multiple state transitions; and

a network management system configured to receive said spontaneously generated notifications.

21. (Original) The system of claim 20, further comprising:

an agent configured to detect the generation of notifications by the network components, and configured to report detected notifications to said network management system.

22. (Previously Presented) The system of claim 21, further comprising:

a state table configured to store said specified states and state transitions, including composite state transitions.

23. (Previously Presented) The system of claim 22, wherein the state table is in a network management system.

24. (Currently Amended) The system of claim 22, wherein the state table is in ~~a~~ one of the one or more network components.

25. (Currently Amended) The system of claim ~~22~~49, wherein the agent is further configured to examine one or more conditions of one or more network components and to query ~~the~~ a state table storing said specified states and state transitions to determine whether the one or more conditions represents an illegal or ~~undesired~~ undesirable state or state transition.

26. (Canceled)

27. (Currently Amended) A computer-based system for capturing illegal and undesired behavior for network components and for interactions between components comprising:

one or more network components;

an agent configured to examine said network components to determine whether specified states or state transitions, including composite state transitions, have occurred,

wherein the agent is configured to generate notifications upon a determination that a specified state or state transition has occurred~~, and~~;

wherein the agent is configured to report detected notifications to a network management system;

wherein each of said composite state transition comprises multiple state transitions;

wherein the specified states and state transitions comprise (1) a set of undesirable states or state transitions associated with undesirable behavior and (2) a set of illegal states or state transitions associated with illegal behavior, said set of illegal states and state transitions being different than said set of undesirable states or state transitions; and

said network management system configured to receive reports of said generated notifications.

28. (Original) The system of claim 27, further comprising:

a state table configured to store said specified states and state transitions, including composite state transitions.

29. (Currently Amended) A computer-readable storage medium carrying one or more sequences of instructions for capturing ~~illegal and undesired~~ behavior for network components and for interactions between components, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

~~specifying~~ accessing first data that defines one or more states and state transitions for ~~one or more components~~ a particular component or ~~interactions~~ interaction between a particular two or more components,

wherein ~~specifying includes specifying~~ the first data defines at least one composite state transition, each of said composite state transition comprising multiple state transitions; and

~~when a~~ in response to the particular component or interaction between ~~a~~ the particular two or more components ~~enters~~ entering a particular state or state transition, generating a notification corresponding to the particular state or state transition,

wherein the particular state or state transition is one of the one or more states ~~or~~ and state transitions.

30. (Previously Presented) The computer-readable storage medium as recited in Claim 29, wherein the one or more states are specified based on thresholds.

31. (Previously Presented) The computer-readable storage medium as recited in Claim 29, wherein said notifications are events.

32. (Previously Presented) The computer-readable storage medium as recited in Claim 29, wherein the particular component or interaction between the particular two or more components is a component, and wherein the step of generating the notification comprises generating the notification by the component.

33. (Currently Amended) The computer-readable storage medium as recited in Claim 29, wherein the particular component or interaction between the particular two or more components is an interaction between the particular two or more components, and wherein the notification is generated by at least one of the ~~the~~ particular two or more components.

34. (Previously Presented) The computer-readable storage medium as recited in Claim 29, wherein the instructions for carrying out the step of creating and storing first information further comprise instructions for carrying out the step of:

reporting the notification to a network management system.

35. (Previously Presented) The computer-readable storage medium as recited in Claim 29, wherein the instructions for carrying out the step of creating and storing first information further comprise instructions for carrying out the steps of:

detecting that the particular component or interaction between the particular two or more components has entered the particular state or state transition; and

wherein said notification is generated in response to said step of detecting.

36. (Currently Amended) The computer-readable storage medium as recited in Claim 35, wherein the step of detecting is performed by an agent, said agent being different than the particular component.

37. (Canceled)

38. (Previously Presented) The computer-readable storage medium as recited in Claim 29, wherein the instructions for carrying out the step of creating and storing first information further comprise instructions for carrying out the step of:

polling the particular component or the particular two or more components to determine that the particular state or state transition has occurred.

39–42. (Canceled)

43. (Currently Amended) The computer-readable storage medium as recited in Claim ~~39~~54, wherein the set of one or more illegal states or state transitions comprises a state

associated with an authorization violation ~~and~~ or an authentication forgery ~~are defined as illegal states~~.

44. (Currently Amended) The computer-readable storage medium as recited in Claim ~~40~~54, wherein the set of one or more undesirable states or state transitions comprises a state associated with a sudden ~~QoS~~ quality of service degradation or a violation of a service level agreement ~~is defined as an undesired state~~.

45. (Previously Presented) The computer-readable storage medium as recited in Claim 29, wherein the instructions for carrying out the step of creating and storing first information further comprise instructions for carrying out the step of examining multiple notifications to deduce one or more trends regarding the network.

46. (Previously Presented) The computer-readable storage medium as recited in Claim 45, wherein the step of examining multiple notifications comprises examining notifications for stable-behavior in a threshold value for a particular trend.

47. (Previously Presented) The computer-readable storage medium as recited in Claim 45, wherein the step of examining multiple notifications comprises examining notifications for increases or decreases in a threshold value for a particular trend.

48. The method recited in claim 1, further comprising:

accessing second data that indicates, for the particular component or interaction between the particular two or more components, a set of one or more undesirable states or state transitions;

wherein each of said one or more undesirable states or state transitions is a state or state transition of the one or more states and state transitions that is associated with undesirable behavior; and

accessing third data that indicates, for the particular component or interaction between the particular two or more components, a set of one or more illegal states or state transitions;

wherein each of said one or more illegal states or state transitions is a state or state transition of the one or more states and state transitions that is associated with illegal behavior;

wherein the set of one or more illegal states is different from the set of one or more undesirable states;

wherein the particular state or state transition belongs to either the set of one or more undesirable states or state transitions or the set of one or more illegal states or state transitions.

49. (New) The system recited in claim 20, wherein the specified states and state transitions comprise (1) a set of undesirable states or state transitions associated with undesirable behavior and (2) a set of illegal states or state transitions associated with illegal behavior, said set of illegal states and state transitions being different than said set of undesirable states or state transitions.

50. (New) The method recited in claim 1, wherein the first data is stored in a state table in a network management system, wherein the step of generating is performed by a component or agent separate from the network management system.

51. (New) The method recited in claim 1, wherein the first data is stored in a state table in the particular component or in at least one of the two or more particular components.

52. (New) The method recited in claim 48, further comprising:

detecting that the particular component or interaction between the particular two or more components has entered the particular state or state transition;

wherein said notification is generated in response to said step of detecting;

wherein the step of detecting comprises:

monitoring a condition associated with the particular component or interaction between the two or more particular components;

querying a state table storing said first data to determine a state for the particular component or interaction between the two or more particular components;

determining, based on the second data and third data, that the determined state belongs to either the set of one or more undesirable states or state transitions or the set of one or more illegal states or state transitions.

53. (New) The method recited in claim 1, wherein the particular state or state transition is a composite state transition.

54. (New) The computer-readable storage medium recited in claim 29, wherein the instructions for carrying out the step of creating and storing first information further comprise instructions for carrying out the steps of:

accessing second data that indicates, for the particular component or interaction between the particular two or more components, a set of one or more undesirable states or state transitions;

wherein each of said one or more undesirable states or state transitions is a state or state transition of the one or more states and state transitions that is associated with undesirable behavior; and

accessing third data that indicates, for the particular component or interaction between the particular two or more components, a set of one or more illegal states or state transitions;

wherein each of said one or more illegal states or state transitions is a state or state transition of the one or more states and state transitions that is associated with illegal behavior;

wherein the set of one or more illegal states is different from the set of one or more undesirable states;

wherein the particular state or state transition belongs to either the set of one or more undesirable states or state transitions or the set of one or more illegal states or state transitions.

55. (New) The computer-readable storage medium as recited in claim 29, wherein the first data is stored in a state table in a network management system, wherein the step of generating is performed by a component or agent separate from the network management system.

56. (New) The computer-readable storage medium as recited in claim 29, wherein the first data is stored in a state table in the particular component or in at least one of the two or more particular components.

57. (New) The computer-readable storage medium as recited in claim 54, wherein the instructions for carrying out the step of creating and storing first information further comprise instructions for carrying out the step of:

detecting that the particular component or interaction between the particular two or more components has entered the particular state or state transition;

wherein said notification is generated in response to said step of detecting;

wherein the step of detecting comprises:

monitoring a condition associated with the particular component or interaction between the two or more particular components;

querying a state table storing said first data to determine a state for the particular component or interaction between the two or more particular components;

determining, based on the second data and third data, that the determined state belongs to either the set of one or more undesirable states or state transitions or the set of one or more illegal states or state transitions.

58. (New) The computer-readable storage medium as recited in claim 29, wherein the particular state or state transition is a composite state transition.